Algebra 2025/2026: Exercise sheet 13

Exercise 1.

Let $K \subset \mathbb{C}$ be the splitting field of $X^4 - 2$ over $\mathbb{Q}$.

Show that $K = \mathbb{Q}[i, \sqrt[4]{2}]$. Conclude that $[K : \mathbb{Q}] = 8$. And finally prove that $K \cap \mathbb{R} = \mathbb{Q}[\sqrt[4]{2}]$.

Exercise 2.

Let p be a prime number and $\zeta_p := exp^{\frac{2i\pi}{p}} \in \mathbb{C}$.

1) Prove that ζ_p has degree $p-1$ over $\mathbb{Q}$. (You may use Ex 3 of sheet 12).

2) Prove that $X^p - 2 \in \mathbb{Q}[X]$ is irreducible.

Let $K \subset \mathbb{C}$ be the splitting field (in $\mathbb{C}$) of $X^p - 2$ over $\mathbb{Q}$.

3) Prove that $K = \mathbb{Q}[\zeta_p, \sqrt[p]{2}]$ and compute $[K : \mathbb{Q}]$.

4) As K is a Galois extension of $\mathbb{Q}$, we know that $\mathbb{Q}[\zeta_p] \subset K$ is also a Galois extension. Show that $Gal(K|\mathbb{Q}[\zeta_p])$ is isomorphic to $\mathbb{Z}/p.\mathbb{Z}$ and give the list of all the conjugates of $\sqrt[p]{2}]$.

Exercise 3.

Let p be a prime number $\neq 2$ and $\zeta_p := exp^{\frac{2i\pi}{p}} \in \mathbb{C}$.

1) Prove that ζ_p has degree $p-1$ over $\mathbb{Q}$. (You may use Ex 3 of sheet 12).

Let $K = \mathbb{Q}[\zeta_p]$.

2) Prove that $cos(\frac{2\pi}{p}) \in K$ and that ζ_p has degree ≤ 2 over $\mathbb{Q}[cos(\frac{2\pi}{p})]$. [Hint: observe that $2cos(\frac{2\pi}{p}) = \zeta_p + (\zeta_p)^{-1}$...]

3) Conclude that for $p > 2$, $cos(\frac{2\pi}{p})$ has degree $\frac{p-1}{2}$ over $\mathbb{Q}$, and give the list of all the conjugates of $cos(\frac{2\pi}{p})$.

Exercise 4.

Let $n \geq 2$ be an integer.

1) We denote by $\phi(n)$ the number a generators of the group $\mathbb{Z}/n.\mathbb{Z}$, in other words, of elements of order n. Let $d|n$ be a divisor of n. Show that the number of elements of order d in the group $\mathbb{Z}/n.\mathbb{Z}$ is $\phi(d)$. Conclude that $\phi(n) = \Sigma_{d|n}\phi(d)$.

2) Let G be a finite group of order n. Assume that for any divisor d of n, the number of elements $x \in G$ such that $x^d = e_G$ is less than d. Show that the number of elements of order d in G is 0 or $\phi(d)$. Conclude that G is cyclic of order n.

3) Let K be a field and let $G \subset K^\times$ be a finite subroup. Show that G is cyclic.